

NAMEPA
Marine Operations in a Disrupted World
The Cyber Challenge: IMO 2021 and Beyond
February 25, 2021

November 5, 2020

Who We Are



Who We Are:

- Trusted Best-in-Class partners
- Technology / vendor agnostic
- Global Reach

What We Offer:

- Enterprise assessment approach - the **HACyberLogix**
- Tailored cyber threat intelligence - informed by “attack side”
- Customized Cyber Training



The Maritime Cyber Risk Landscape

Where are we headed now

Cyber Risk Management and the IMO

*Industry was struggling to both accept the risks of cyber...
and qualify and quantify those risks.*

Now there is specific guidance on how to address risk

Resolution MSC.428 (98) Maritime Cyber Risk Management in Safety Management Systems affirms that:

- *Approved Safety Management Systems should take cyber risk management into account in accordance with the objectives and requirements of the ISM Code.*
- ***Existing risk management practices*** *should be used to address the operational risks associated with the growing dependence on cyber enabled systems.*

Involved Industry Organizations





IMO 2021 What now?

Change in industry guidance from general to more specific

Now that IMO has provided direction companies can start organizing. They must:

- 1. Meet the regulation*
- 2. Put into practice the risk management principles of ISM as apply to Cybersecurity*

A daunting task!

Lots to do!

NIST Cybersecurity Framework Functional Category	NIST CSF Category	IMO Clause (Category)	IMO Clause Description (Clause 3.5)
Identify	- Asset Management - Business Environment - Governance - Risk Assessment - Risk Management Strategy	Identify (3.5.1)	Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations 2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners. 2.2.3 These Guidelines are recommendatory. 3. ELEMENTS OF CYBER RISK MANAGEMENT 3.1 For the purpose of these Guidelines, cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. 3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks. 3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms. 3.4 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework. 3.5 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations. 3.5.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations. 3.5.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations. 3.5.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner. 3.5.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event. 3.5.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.
Protect	- Access Control - Awareness & Training - Data Security - Information Protection Processes & Procedures - Maintenance - Protective Technology	Protect (3.5.2)	Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber event 3.5.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
Detect	- Anomalies & Events - Security Continuous Monitoring - Detection Processes	Detect (3.5.3)	Detect: Develop and implement activities necessary to detect a cyber event in a timely manner. 3.5.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
Respond	- Response Planning - Communications - Analysis - Mitigation - Improvements	Respond (3.5.4)	Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event. 3.5.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
Recovery	- Recovery Planning - Improvements - Communications	Recover (3.5.5)	Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber event. 3.5.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Now you have a long list of things to do



What and how?

Implementation is different than meeting IMO 2021 on paper

- Prioritize action items
 - What can we do and when do we need help?
- Develop a system to support ongoing activities
 - Establish KPIs and monitor leading and lagging indicators

Reality...There are Challenges

The reality is that challenges exist. The implementation of cybersecurity best practices requires:

- Money
- *Time*
- *Personnel*
- *Skill sets*
- *Leadership*

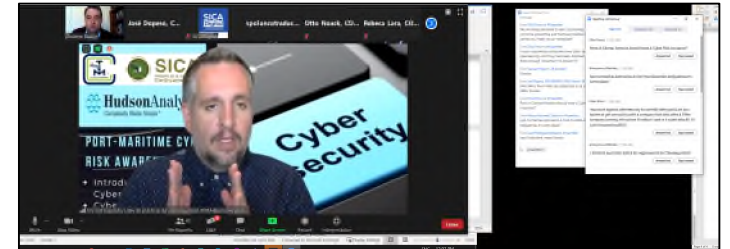
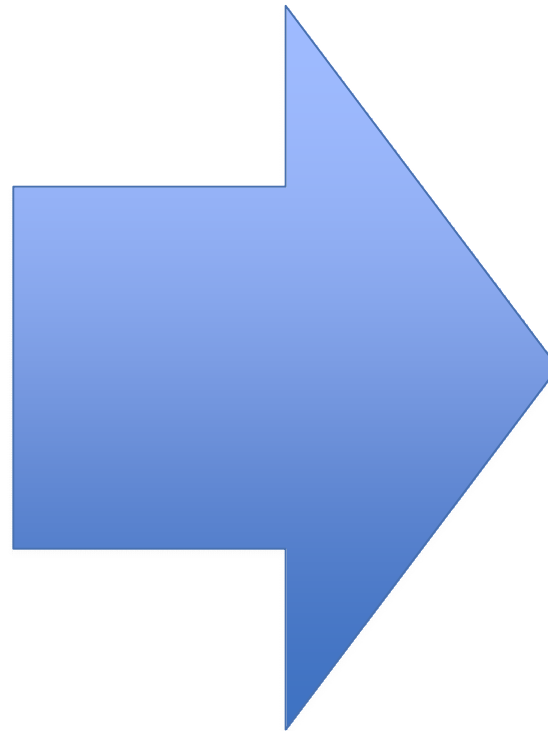
Supporting Resources

Resources	Information	Implementation Support
Internal resources	Yes	Yes
Industry Organizations	Yes	
Legal	Yes	
Insurer	Yes	Maybe
Service providers	Yes	Yes
Information sharing and analysis Center (ISAC)	Yes	Yes
Threat Intelligence services	Yes	Yes
Cyber response organizations	Yes	Yes
Government	Yes	

The World is Changing... Fast



Where we were...



....Where we're going

How Hudson is Responding...



2021 CYBER COMPLIANCE

MARITIME CYBERSECURITY ASSISTANCE IN
UPGRADING SAFETY MANAGEMENT SYSTEMS
TO COMPLY WITH THE IMO 2021 MANDATE

HUDSONCYBER
A DIVISION OF HUDSONANALYTIX, INC.
FERRY TERMINAL BUILDING
SUITE 300
#2 AQUARIUM DRIVE
CAMDEN, NJ 08103
USA

WWW.HUDSONCYBER.COM



HACYBERLOGIX

FACILITATING AND SUSTAINING CYBERSECURITY
CAPABILITIES FOR MARITIME TRANSPORTATION
COMPANIES AROUND THE WORLD

HUDSON - CYBER
FERRY TERMINAL BUILDING
SUITE 300
#2 AQUARIUM DRIVE
CAMDEN, NJ 08103 USA

WWW.HUDSONCYBER.COM



CYBERHELM™

PREEMPTIVE CYBER THREAT PROTECTION
DESIGNED FOR THE MARITIME INDUSTRY

HUDSONCYBER
A DIVISION OF HUDSONANALYTIX, INC.
FERRY TERMINAL BUILDING
SUITE 300
#2 AQUARIUM DRIVE
CAMDEN, NJ 08103
USA

WWW.HUDSONCYBER.COM



Thank You!



1800 Chapel Avenue West
Suite 360
Cherry Hill, NJ 08002

Office: +1.856.342.7500
Mobile: +1.609.505.6878
Email: cynthia.hudson@hudsonanalytix.com

Cynthia A. Hudson
Founder & CEO

Parting Thoughts: Key Takeaways for Maritime Stakeholders Right Now



ORGANIZE!

Establish multi-disciplined cyber working group that meets regularly. Grant authorities!



ENTERPRISE ASSESSMENT

Perform an enterprise level cybersecurity capability assessment. Discover what you have.



DEVELOP AN INVENTORY

Develop an inventory of your assets. Classify critical systems.



QUANTIFY YOUR EXPOSURE

Identify your most valuable assets, determine values and develop loss scenarios. Prioritize.



STRESS TEST YOUR INSURANCE

Review all policies for gaps/exclusions. How do they perform against the loss scenarios?



PREPARE

Establish a Cyber Incident Response (IR) plan. Update Data Loss Prevention (DLP), Disaster Recovery (DR) and Business Continuity (BC) Plans.



TRAIN

Train! Deliver awareness training to executives (first) then staff and crews. Incorporate cyber risk factors into drills and exercises.



SUSTAIN RESOURCES

Develop and sustain resources (people, processes, tools) with a budget.